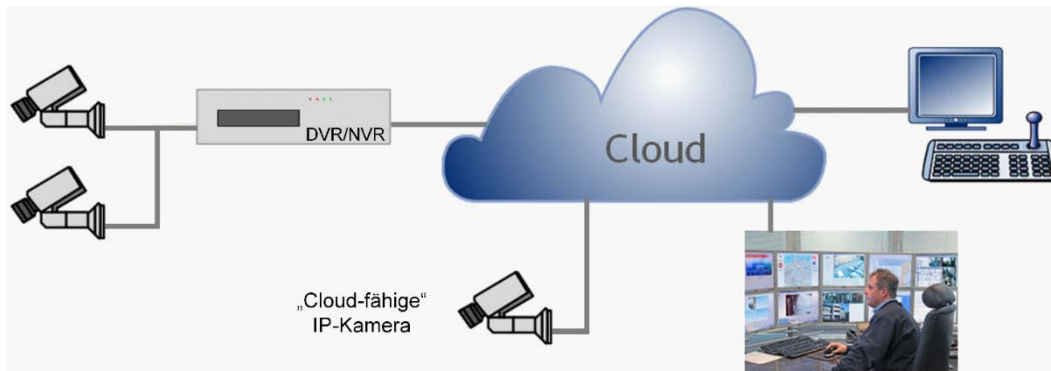


Videosicherheit in der Cloud

Brücken, 28.08.2020

Die Nutzung von Cloud-Diensten zur Speicherung von Videodaten ist ein aktueller Trend in der modernen Videosicherheitstechnik. Anwender können aus einem immer größer werdenden Angebot interessanter Dienstleistungen für dieses Spezialgebiet auswählen.

Bei der Nutzung von Cloud-basierten Lösungen wird ein Teil der Videosicherheitsinfrastruktur nicht mehr selbst betrieben, sondern von einem oder mehreren Cloud-Anbietern angemietet. Die Speicherung und Auswertung der aufgezeichneten Bilder oder weiterer Daten kann auf diesem Wege ausgelagert werden. Die Übertragung erfolgt über eine Internet-Verbindung.



Der Anbieter des Cloud-Dienstes kann ein externer Anbieter („**Public-Cloud**“) oder das eigene, i.d.R. größere, Unternehmen sein („**Private-Cloud**“). Zudem existieren diverse Mischformen. Bei allen Varianten stellt der Cloud-Dienste-Anbieter die für seine Leistungen notwendige Hard- und Software zum Betreiben der Cloud zur Verfügung. Die videospezifische Software liefert nach wie vor der Hersteller der Videosicherheitslösung.

Vorteile und Herausforderungen

Für den Betreiber der Videosicherheitsanlage bieten sich bei der Nutzung von Public-Cloud-Lösungen Kosteneinsparpotenziale, da der Aufwand für die Beschaffung, den Betrieb und die Wartung geeigneter Geräte entfällt. Stattdessen genügt die Zahlung einer vergleichsweise geringeren Gebühr. Schutzbedürftige Unternehmen profitieren somit auch von den niedrigeren Anfangsinvestitionen und dem geringeren Bedarf an eigenem technischem Know-how. Ein weiterer Vorteil ist die einfache Erweiterbarkeit der Anlage. Zusätzliche Kameras lassen sich i.d.R. ohne hardwarespezifische Einschränkungen hinzufügen. Durch die Spezialisierung des Cloud-Anbieters ist mit höheren Wartungsintervallen und dem Einsatz mehrerer Server zu rechnen. Somit kann eine höhere Systemzuverlässigkeit erreicht werden, als dies der Betreiber der Videosicherheitsanlage selbst erreichen kann.

Nachteilig ist jedoch die Abhängigkeit vom jeweiligen Dienste-Anbieter, mit dem unter Umständen ein mehrjähriges Vertragsverhältnis eingegangen werden muss. Das Übertragen der sensiblen Daten erfordert zudem ein hohes Maß an Vertrauen. Der genaue Speicherort ist nur in den seltensten Fällen bekannt. Stehen die Server im Ausland, muss unbedingt auf die Vereinbarkeit des auswärtigen Datenschutzes mit der Gesetzeslage in Deutschland geachtet werden.

Veränderungen der Allgemeinen Geschäftsbedingungen, der Preise oder der Soft- und Hardware auf Seiten des Anbieters bergen ein zusätzliches Risiko.

Rechtslage bei Nutzung einer Public-Cloud

Innerhalb der professionellen Videosicherheitstechnik werden in den meisten Fällen personenbezogene Daten, wie Kamerabilder von Kunden, Lieferanten und Mitarbeitern, erhoben, verarbeitet und genutzt. Hierbei greifen automatisch die Regelungen des Bundesdatenschutzgesetzes (BDSG) und der Datenschutzgrundverordnung (DSGVO), die seit Mai 2018 verbindlich gilt.

Beide Vorschriften sind zwingend auch bei Nutzung einer Public-Cloud zu beachten. Daher sollte die Auswahl des Cloud-Dienste-Anbieters sehr sorgfältig erfolgen. Dieser sollte dem Auftraggeber die Einhaltung der in den gültigen Gesetzen aufgeführten Anforderungen rechtsverbindlich zusichern und die übertragenen Daten ausschließlich auf Servern innerhalb der EU speichern. Nach Bundesdatenschutzgesetz ist der Betreiber der Videosicherheitsanlage für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich (BDSG § 62 Abs. 1). Dies bedeutet praktisch, dass die Videodaten, die beim Cloud-Dienste-Anbieter gespeichert werden, noch immer im Eigentum des Betreibers der Videoanlage sind. Damit ist der Betreiber im juristischen Sinne die „verantwortliche Stelle“. Dementsprechend ist nicht davon auszugehen, dass im Falle eines Datenmissbrauchs der Cloud-Dienste-Anbieter haftbar gemacht werden kann; vielmehr ist der Betreiber der Videoanlage haftbar. Für die Betreiber der Videosicherheitsanlage ist eine rechtliche Beratung bzw. juristische Vertragsprüfung im Vorfeld unbedingt zu empfehlen.

Außerdem besteht lt. DSGVO die Notwendigkeit des Abschlusses eines Auftragsverarbeitungsvertrages zwischen dem Betreiber und dem Cloud-Anbieter. Der Cloud-Anbieter muss sich darin zur Einhaltung der Vorgaben der DSGVO verpflichten.

Datensicherheit in der Cloud

Eine besondere Herausforderung ist die Sicherheit der Daten in der Public-Cloud. Die übertragenen Videoströme dürfen in keinem Fall zugänglich für Unbefugte sein. Sie sollten daher verschlüsselt übertragen und gespeichert werden. Dies gilt sowohl für die kompletten Videoströme als auch alle zusätzlichen Informationen über die Merkmale der Daten selbst (Metadaten). Nur so lassen sich diese wirksam gegen Hackerangriffe schützen. Für die Analyse der Bilddaten in der Cloud ist dann eine „cloud-fähige“ Auswertesoftware notwendig, die eine entsprechende Entschlüsselung vornehmen kann.

Die Verwendung einer Private-Cloud, die vom eigenen Unternehmen betrieben wird, ist hier eine sicherere Alternative. Sie lässt sich zentral an einem oder verteilt an mehreren Standorten betreiben. Die Daten sind über das firmeneigene Intranet oder eine VPN-Verbindung abrufbar, wodurch nur die Teilnehmer dieses Netzwerkes Zugriff auf die Daten haben. Das Unternehmen hat somit selbst die Kontrolle über die Hard- und Software sowie die gespeicherten Informationen. Datensicherheit und Datenschutz können hierdurch den eigenen Maßstäben angepasst werden. Durch eine räumlich getrennte, redundante Speicherung lässt sich die Sicherheit weiter erhöhen.

Marktentwicklung von Cloud-basierten Videosicherheitssystemen

Obwohl viele Unternehmen im Bereich der allgemeinen IT zunehmend auf die Verwendung von Cloud-Diensten setzen, ist der Marktanteil Cloud-basierter Videosicherheitssysteme bisher noch eher gering. Dieser dürfte in den kommenden Jahren jedoch deutlich steigen.

Bei der Betrachtung der Marktentwicklung ist allerdings zwischen Lösungen für Unternehmen und private Haushalte zu unterscheiden. Im Bereich der Home-Security bieten bereits viele Hersteller einfach zu installierende Kameras, die sich über das eigene Heimnetz direkt mit der Cloud verbinden lassen. Videoaufnahmen können auf diesem Wege problemlos abgespeichert und bei Bedarf wiedergegeben werden, bspw. via App auf Smartphones oder Tablets. Die professionelle Videosicherheitstechnik, wie sie etwa in öffentlich zugänglichen Bereichen oder auf dem Privatgelände von Unternehmen zum Einsatz kommt, stellt jedoch weitaus höhere Anforderungen an die Cloud-Dienste. Zu beachten sind hierbei vor allem die deutlich größeren Datenmengen und (datenschutz-) rechtlichen Aspekte. Diese bremsen die fortschreitende Nutzung von Cloud-Diensten aus. Insbesondere das aufkommende Datenvolumen ist eine technische Herausforderung. Beispielsweise kann eine 2-Megapixel-Kamera, je nach Komplexität der Szene, in 24 Stunden eine Datenmenge zwischen 25 und 100 Gigabyte produzieren. Bei einer 8-Megapixel-Kamera sind es in 24 Stunden schon 50 - 200 Gigabyte.

Vor dem Hintergrund, dass eine Videosicherheitsanlage bspw. aus sechs oder mehr Kameras besteht, wird schnell deutlich, dass eine Übertragung der Daten in Echtzeit nur schwer realisierbar ist.

Auch zukünftig gilt es deshalb, die Datenmengen durch eine Begrenzung der Bilder pro Sekunde, eine ereignisgesteuerte Aufzeichnung oder eine reduzierte Bildauflösung zu verringern.

Der Fachausschuss Video im BHE Bundesverband Sicherheitstechnik e.V. beschäftigt sich mit allen aktuellen Themen der Videotechnik. Die Hersteller, Planer und Errichter der Videosicherheit haben sich zum Ziel gesetzt, den sehr dynamischen Technologiefortschritt dieser Branche für alle Marktteilnehmer transparent darzustellen.

Aktuelle Aspekte der Videosicherheit greift auch der BHE-Praxis-Ratgeber Videosicherheit auf. In diesem rund 200 Seiten starken Nachschlagewerk finden Errichter, Planer, Anwender und Behörden alle wichtigen und notwendigen Informationen. In verständlicher Art und Weise werden die Möglichkeiten und Grenzen moderner Videosicherheit umfassend erläutert.

Nähere Informationen unter www.bhe.de und in der BHE-Geschäftsstelle (info@bhe.de; 06386 9214-0).